ABSTRACT

A method for providing a proactive security in proactive operating environment. The proactive operating environment includes a group of proactive servers communicating over a network. Each proactive server (PS_I) includes a storage that includes a non erasable part that stores a public, non proactive related, key V^I_{Start}. The storage further includes an erasable part for storing private and public data. The proactive server has a discardable one-time private key S^I_{Start} that corresponds to the public key V^I_{Start}. The proactive server further has configuration data C. There is further provided a processor for providing a proactive services to applications. The proactive server has a group public proactive key V_{CERT}, common to the group of proactive servers and a share S^I_{CERT} of a corresponding private proactive key S_{CERT}. The method further includes the steps of invoking initialization procedure for generating restore related information, and invoking a restore procedure for utilizing the public, non proactive related, key V^I_{Start} and the restore related information for restoring the public proactive key V_{CERT}.